Log Analysis of Estonian Internet Voting 2013–2015

Sven Heiberg[1] Arnis Parsovs[23] Jan Willemson[24]

[1]Smartmatic-Cybernetica Centre of Excellence for Internet Voting

[2]Software Technology and Applications Competence Centre

[3]University of Tartu, Institute of Computer Science

[4]Cybernetica

November 5, 2015

European Union
Regional Development Fund

Investing in your future

Research objective

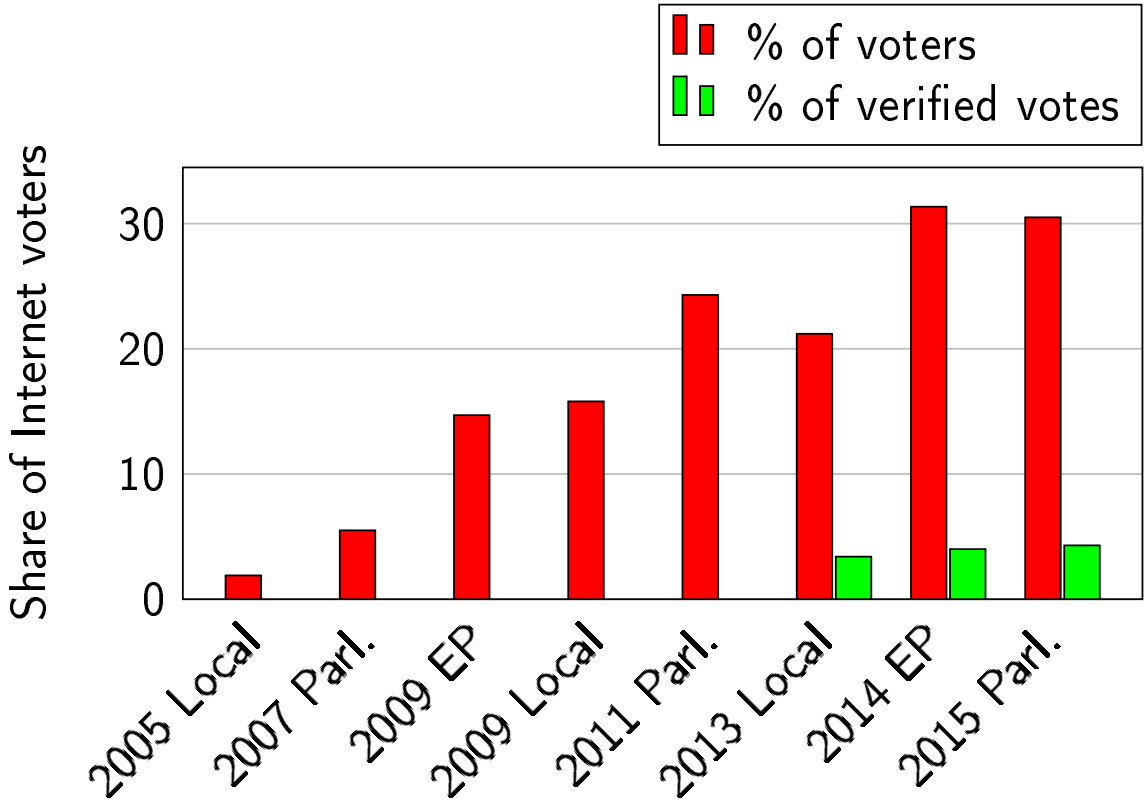
Analyse information available to NEC in order to:

- Detect attacks against i-voting
- Detect system malfunction
- Study voter behaviour

Data sources:

- Log files produced by i-voting servers
- Support requests handled by NEC
- Public information

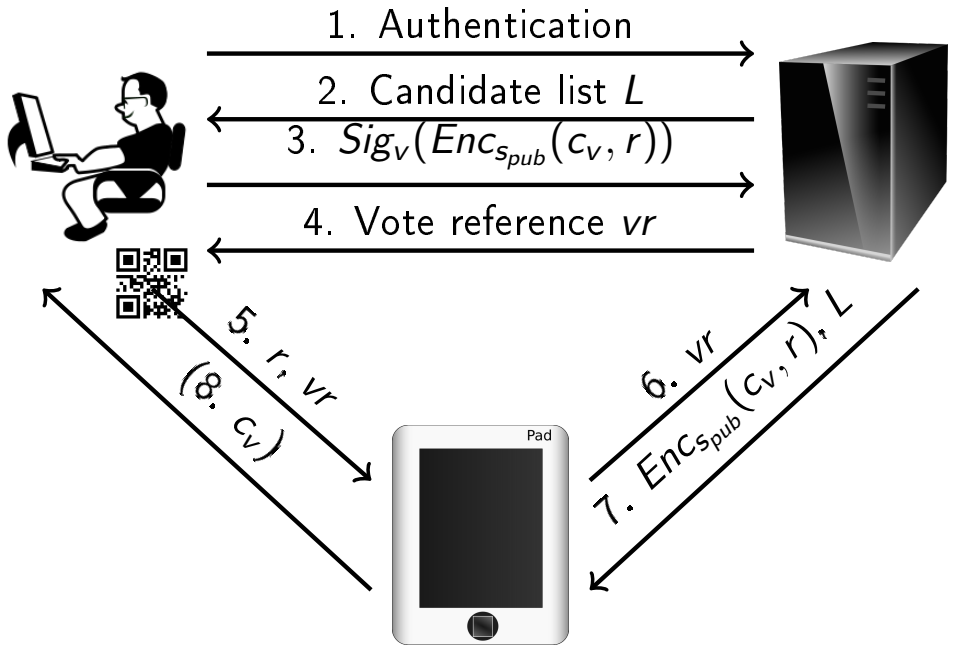
Estonia has i-voted since 2005



Objects of this study:

- Municipal Elections 2013 (KOV2013)
- European Parliament Elections 2014 (EP2014)
- Riigikogu Elections 2015 (RK2015)

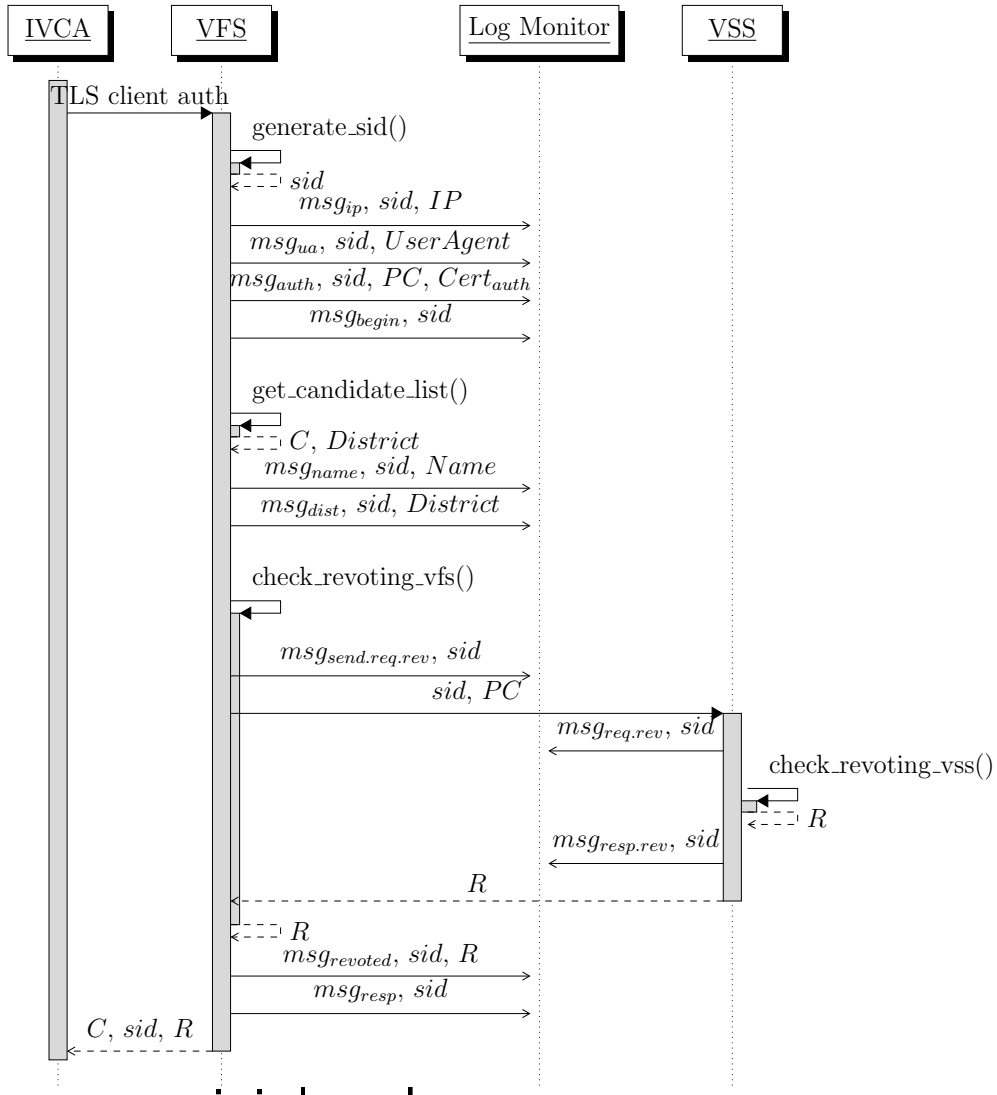
Voting protocol in 2015



There are three sub-protocols:

- Voting with smart card-based eID
- Voting with Mobile-ID
- Vote verification with the mobile device

Logs generated on candidate list retrieval



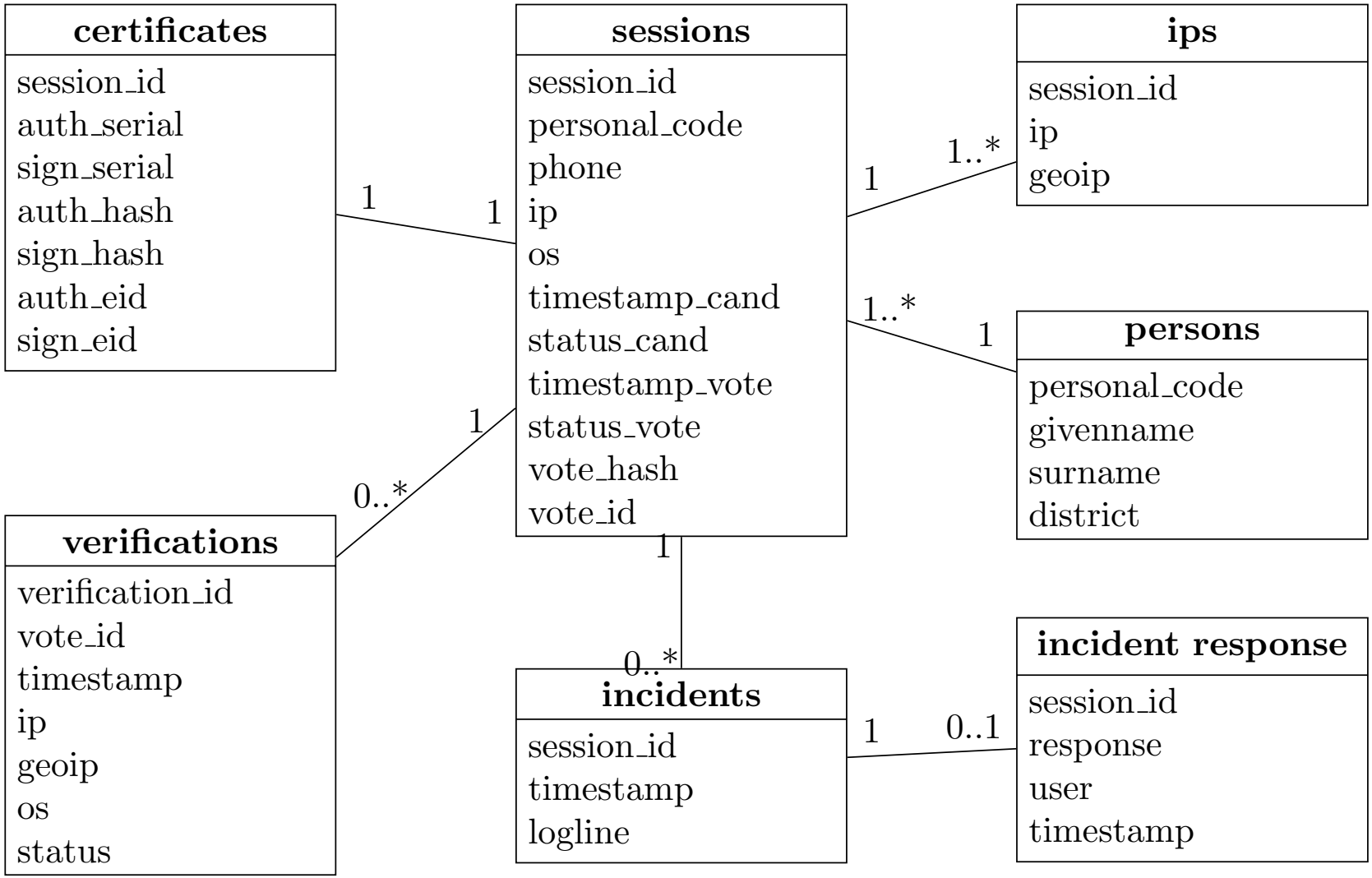
Log analysis is not a trivial task

- Logs in KOV2013 – more than 4'000'000 loglines, 700MB

Log monitor

- Centralized logserver using rsyslog
- Log-processor
  - Parse entry, extract information, fill database
- Analysis front-end
  - Provide descriptive statistics and pattern analysis
- Pseudonymization of logs for later research

Database model



What should we look for in the data?

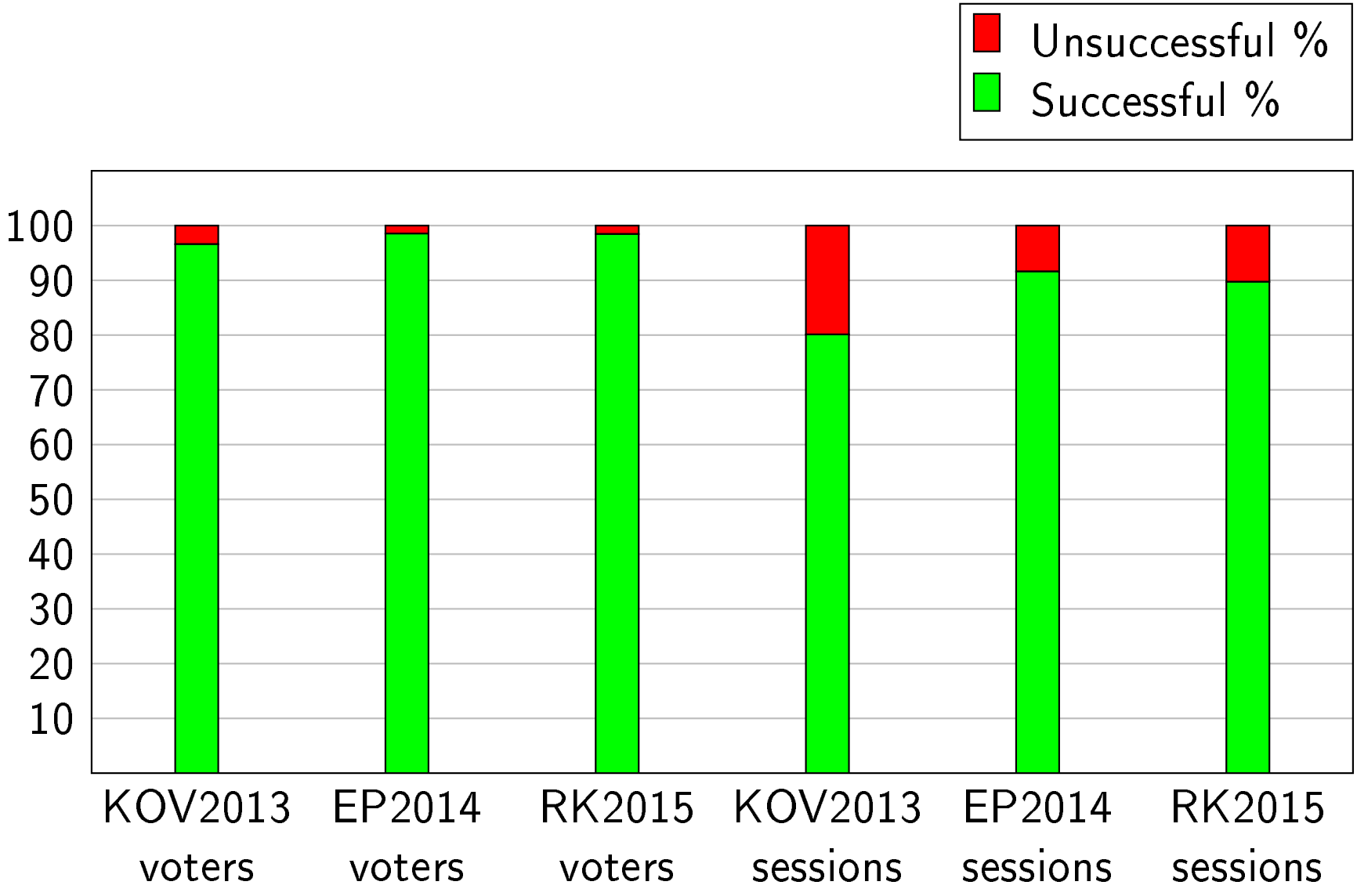
Normality profile:

- Describe in detail "normal" i-voting:
  - The voting session creates only expected log entries
  - The voting session ends with a successfully cast vote
  - The verification session ends with a successfully verified vote
  - The voting session is completed in a few minutes
  - Not too many voters share the same voting IP address
  - Not too many verifiers share the same verifying IP
  - The overall percentage of revoters is small
  - The vote is verified from a single IP address
  - etc.
- In total 24 features
- Anomaly pattern – inverse of normality

Session breakdown

	KOV2013		EP2014		RK2015	
Session kind	Sessions	Voters	Sessions	Voters	Sessions	Voters
All sessions	176,144	–	120,503	–	211,215	–
Voting	170,801	138,532	114,792	104,679	201,811	179,262
Successful	80.1%	133,808	91.6%	103,151	89.7%	176,491
ID card	91.4%	122,471	89.0%	91,964	87.8%	155,267
Mobile-ID	8.6%	11,395	11.0%	11,226	12.2%	21,307
Unsuccessful	19.9%	19,705	8.4%	6,050	10.3%	15,007
ID card	76.9%	16,201	64.9%	4,157	69.1%	11,226
Mobile-ID	23.1%	3,658	35.1%	1,940	30.9%	3,864
Verification	5,343	4,542	5,711	4,250	9,404	7,563
Successful	94.0%	4,521	85.7%	4,210	89.7%	7,522
Unsuccessful	6.0%	84	14.3%	131	10.3%	120

Unsuccessful voting sessions



Unsuccessful voting sessions – explicit errors

Reason for failure	KOV2013	EP2014	RK2015
Explicit error	8,979	4,032	5,513
Common error	1,103	369	1,509
Maintenance	11	0	1
Under-aged voter	28	16	30
Ineligible voter	1,063	315	507
Voting ended	1	38	89
Session expired	–	–	882
Certificate issue	1,978	302	641
Pre-2011 Mobile-ID user	1,490	549	366
Bad Mobile-ID number	2,051	491	974
DigiDocService failure	47	0	0
Mobile-ID failures	2,217	1,148	1,956
Incident	93	1,173	67

Unexpected log entries – incidents

- KOV2013
  - 37 failed ID card sessions – buggy OpenSC
  - 36 failed voting sessions – problematic backup routine
  - 17 malformed votes – lack of error checking in voting client
  - 3 invalid cell numbers – lack of input validation in voting client
- EP2014
  - 1131 failed voting sessions – timezone bug in cert verification
  - 42 incidents with buggy OpenSC or failed M-ID
  - 196 malformed vote verification requests – iOS verification application
  - 5 ID card sessions with card switching
  - 6 sessions with incorrect session state change
- RK2015
  - 1 failed session – inaccessible voter list
  - 2 ID card sessions with card switching
  - 4 ID card sessions vote signature invalid
  - 1 ID card session with invalid certificate signature
  - 59 Mobile-ID sessions using outdated voting client
  - 615 verification sessions using outdated verification application
  - 19 sessions with incorrect session state change

Other reasons for failure

	KOV2013		EP2014		RK2015	
Reason for failure	Sessions	Voters	Sessions	Voters	Sessions	Voters
Other reason	24,969	16,087	5,593	4,340	15,214	12,072
Discontinued (Mobile-ID)	826	595	672	477	1,454	1,039
Authentication	636	470	461	332	1,008	731
Signing	190	178	211	196	446	415
Abnormal	40	34	0	0	0	0
Vote not submitted	24,103	15,563	4,921	3,889	13,760	11,103
ID card	23,004	14,630	4,524	3,521	12,283	9,779
Mobile-ID	1,099	954	397	371	1,477	1,353

Unsuccessful voting sessions – failure to cast a vote

- Abandoned voting sessions – candidate list is successfully downloaded, but the vote is never cast
- Forgotten PIN to access the signing key
- Bugs in voting client (KOV2013)
- Probably not disenfranchisement attack – would be noticed by verification

KOV2013			EP2014			RK2015		
Sessions	Voters	Voters (u)	Sessions	Voters	Voters (u)	Sessions	Voters	Voters (u)
24,103	15,563	2,889	4,921	3,889	869	13,760	11,103	1,947

Verification errors

	KOV2013		EP2014		RK2015	
Reason for failure	Sessions	Verifiers	Sessions	Verifiers	Sessions	Verifiers
Unsuccessful sessions	319	84	787	106	965	218
Newer vote cast	19	6	11	6	17	6
Verification count exceeded	144	47	317	81	154	63
Verification time exceeded	95	54	78	39	121	63
Vote ID not issued	60	–	185	–	58	–
Abnormal state	1	1	–	–	–	–
Malformed vote ID	–	–	196	–	–	–
Invalid verification request	–	–	–	–	615	104

Support requests

Topic	KOV2013	EP2014	RK2015
QR code focussing problems	8	8	0
State-revoked ID cards (issued in 2011)	5	1	0
Android VVA crash	3	1	0
Outdated ID-software, drivers	9	6	8
IVCA Internet connectivity issues	109	24	0
Unsupported voting platforms	3	0	101
Pre-2011 Mobile-ID user	6	2	2
PIN code issues	3	9	0
ID-software not installed	13	0	0
IVCA errors 0xX	13	0	0
MacOS X without ID-software	0	41	0
Website related	0	14	12
Certificates not yet valid bug	0	10	0
iOS-based VVA 0-byte bug	0	4	0
ID-card certificates expired	0	0	2
General election questions	0	0	22
Built-in card readers, drivers	0	0	75
Other	85	49	109

IP address shared by several voters

On average one IP shared by:

- KOV2013: 1.95 voters
- EP2014: 1.97 voters
- RK2015: 2.11 voters

IP addresses shared by more than 100 voters:

- KOV2013: 28 IPs (top IP shared by 1,127 voters)
- EP2014: 22 IPs (top IP shared by 970 voters)
- RK2015: 28 IPs (top IP shared by 1,415 voters)

IP address shared by several voters

- Activity not evenly distributed over the voting period
  - short interval (<5 minutes)
  - the same OS
  - no overlapping sessions
  - IP activity in 24 hours

Group size	KOV2013	EP2014	RK2015
2	8,476	6,033	10,795
3	697	523	1,045
4	108	60	150
5	15	9	15
6	3	1	1
7	0	0	1

- RK2015 7 voter group: Colombian IP, ID cards, 20 minutes
- This is a technical upper-bound to group-voting

IP address shared by several verifiers

On average one IP shared by:

- KOV2013: 1.35 verifiers
- EP2014: 1.31 verifiers
- RK2015: 1.4 verifiers

Top IPs shared by:

- KOV2013: 10 verifiers
- EP2014: 13 verifiers
- RK2015: 11 verifiers

Voting and verification IP the same:

- KOV2013: 53.28%
- EP2014: 56.82%
- RK2015: 60.17%

Large percentage of revoters

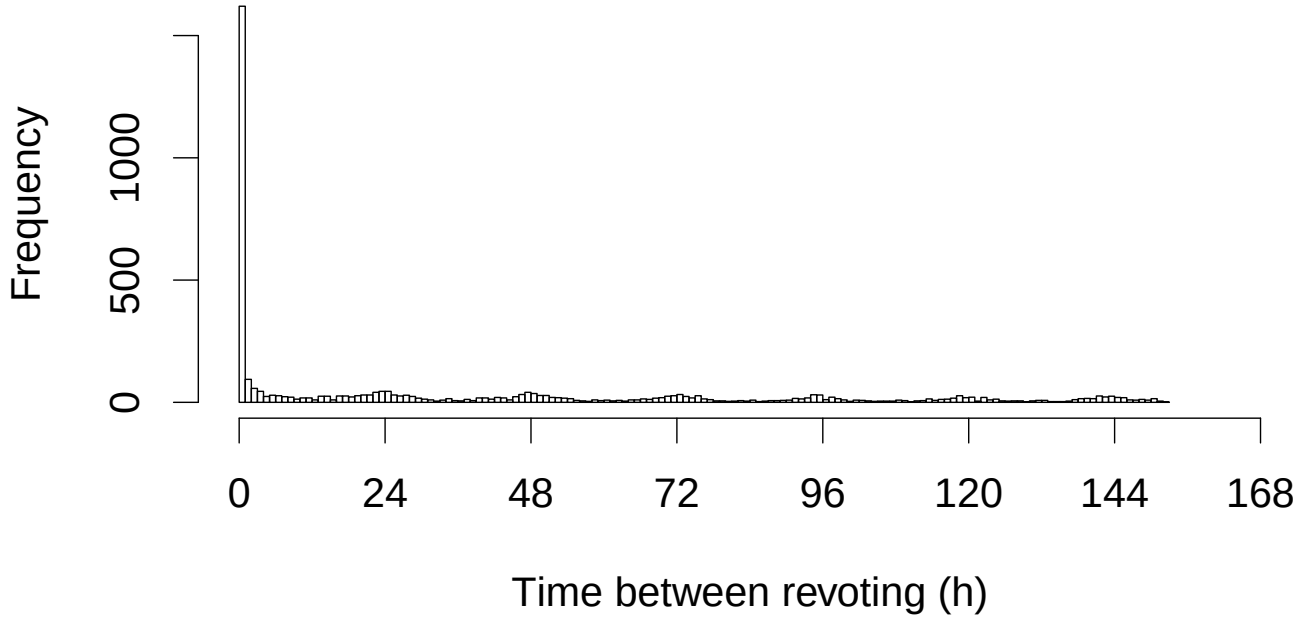
Voters casting more than one vote:

- KOV2013: 1.93% (2,586 voters)
- EP2014: 1.69% (1,743 voters)
- RK2015: 2.29% (4,034 voters)

KOV2013	EP2014	RK2015
32	41	60
27	39	37
10	36	29
10	28	19
9	20	12
8	17	11
8	11	10
7	9	10
6	7	8
6	7	8

Top 10 revoters

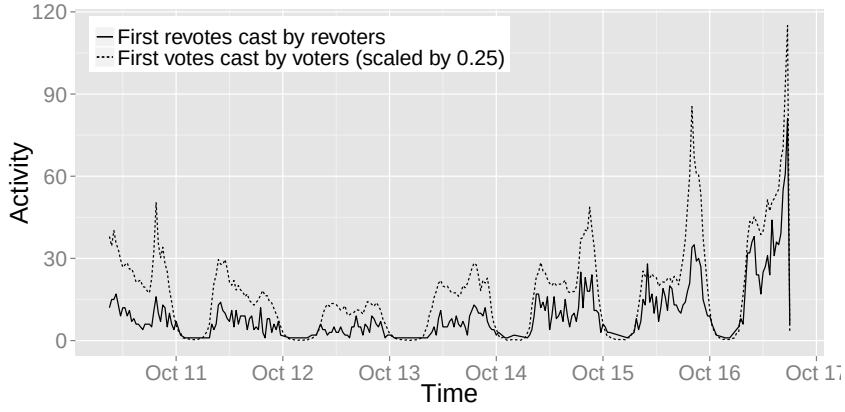
Large percentage of revoters



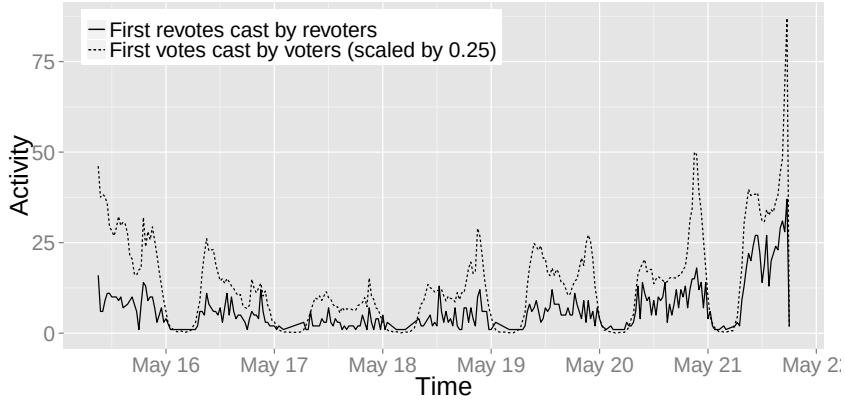
RK2015

- 30% revote in the first ten minutes
- 40% revote in the first hour
- 20% revote from a different IP
- Voters with parallel voting sessions:
  - KOV2013: 60 voters
  - EP2014: 28 voters
  - RK2015: 99 voters

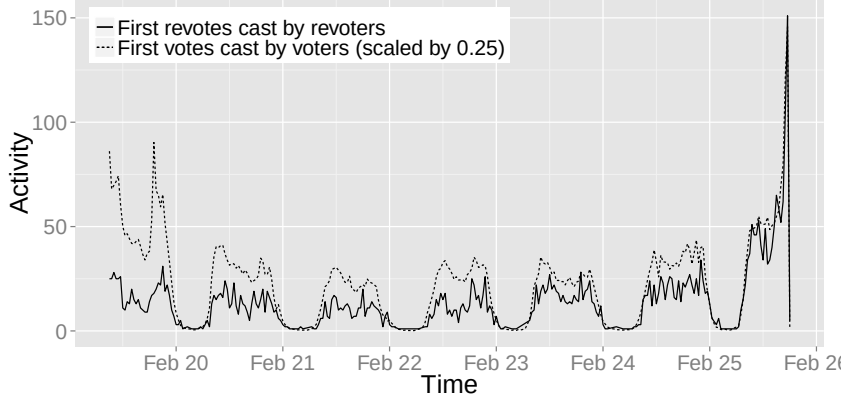
Large percentage of revoters



KOV2013

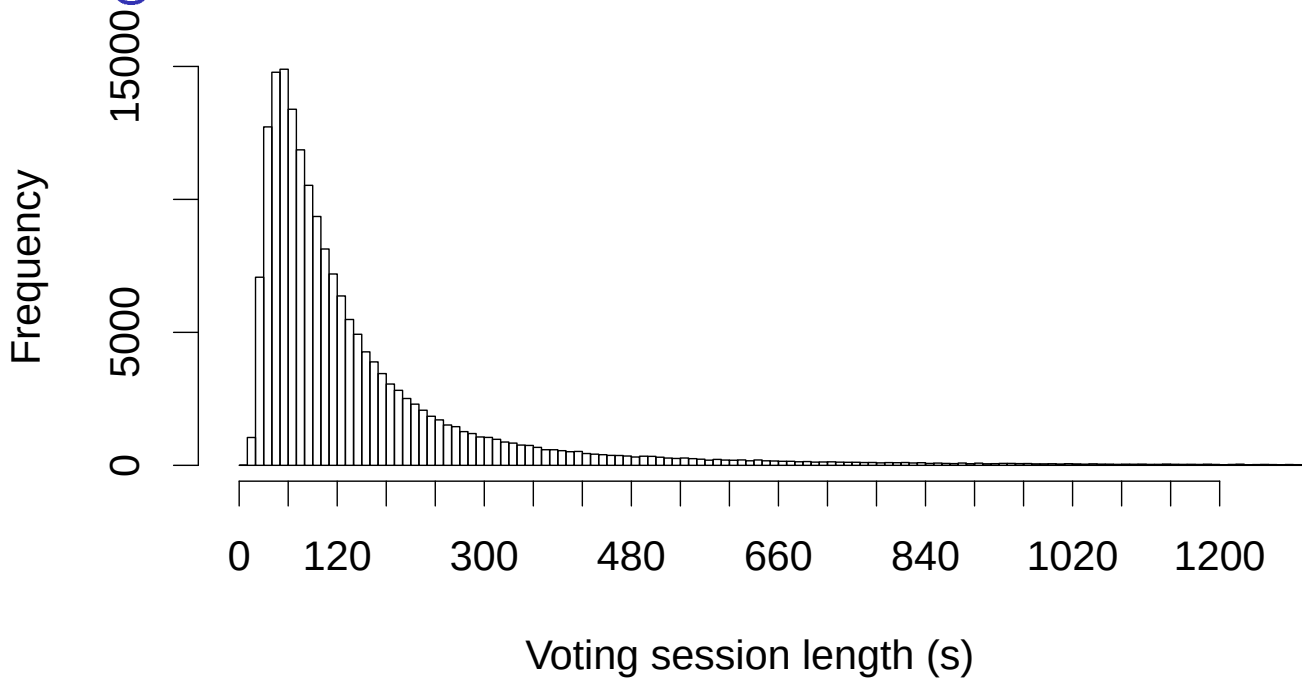


EP2014



RK2015

Voting sessions too slow



RK2015

More than 50% sessions shorter than two minutes

More than 90% sessions shorter than six minutes

The longest voting sessions:

- KOV2013: 4.72 days
- EP2014: 5.6 days
- RK2015: 5.5 days (unsuccessful)

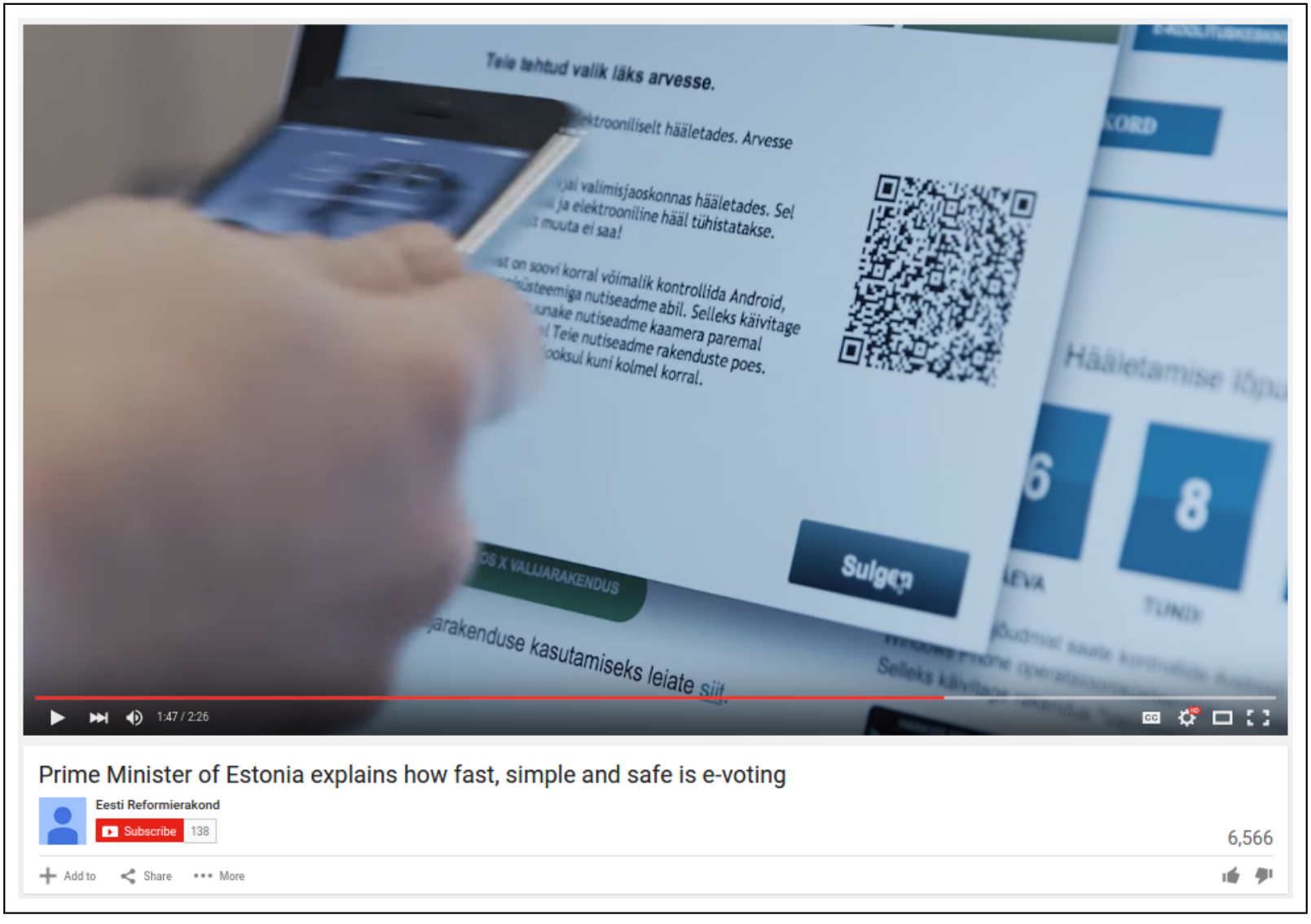
Vote verified from different IP addresses

Votes verified from more than one IP address:

- KOV2013: 19
  - 2 IPs (18)
  - 3 IPs (1)
- EP2014: 23
  - 2 IPs (23)
- RK2015: 49
  - 2 IPs (44)
  - 3 IPs (2)
  - 4 IPs (1)
  - 7 IPs (1)
  - 8 IPs (1)

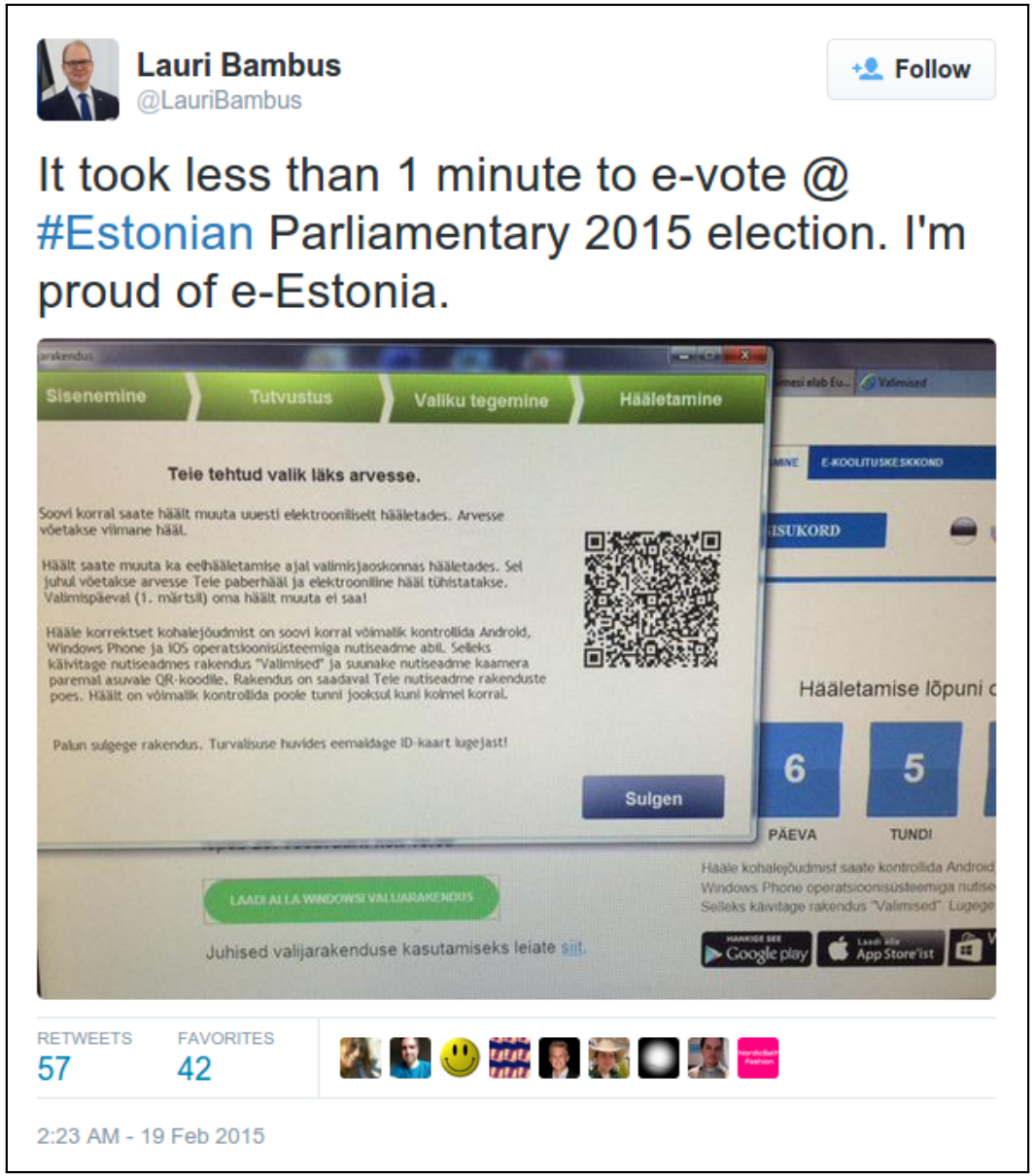
Verifications over several days from different OSs
$\Rightarrow$ QR codes published somewhere!

Vote verified from different IP addresses – RK2015 4 IPs



https://www.youtube.com/watch?v=yZ4s95lFkk4#t=107

Vote verified from different IP addresses – RK2015 8 IPs

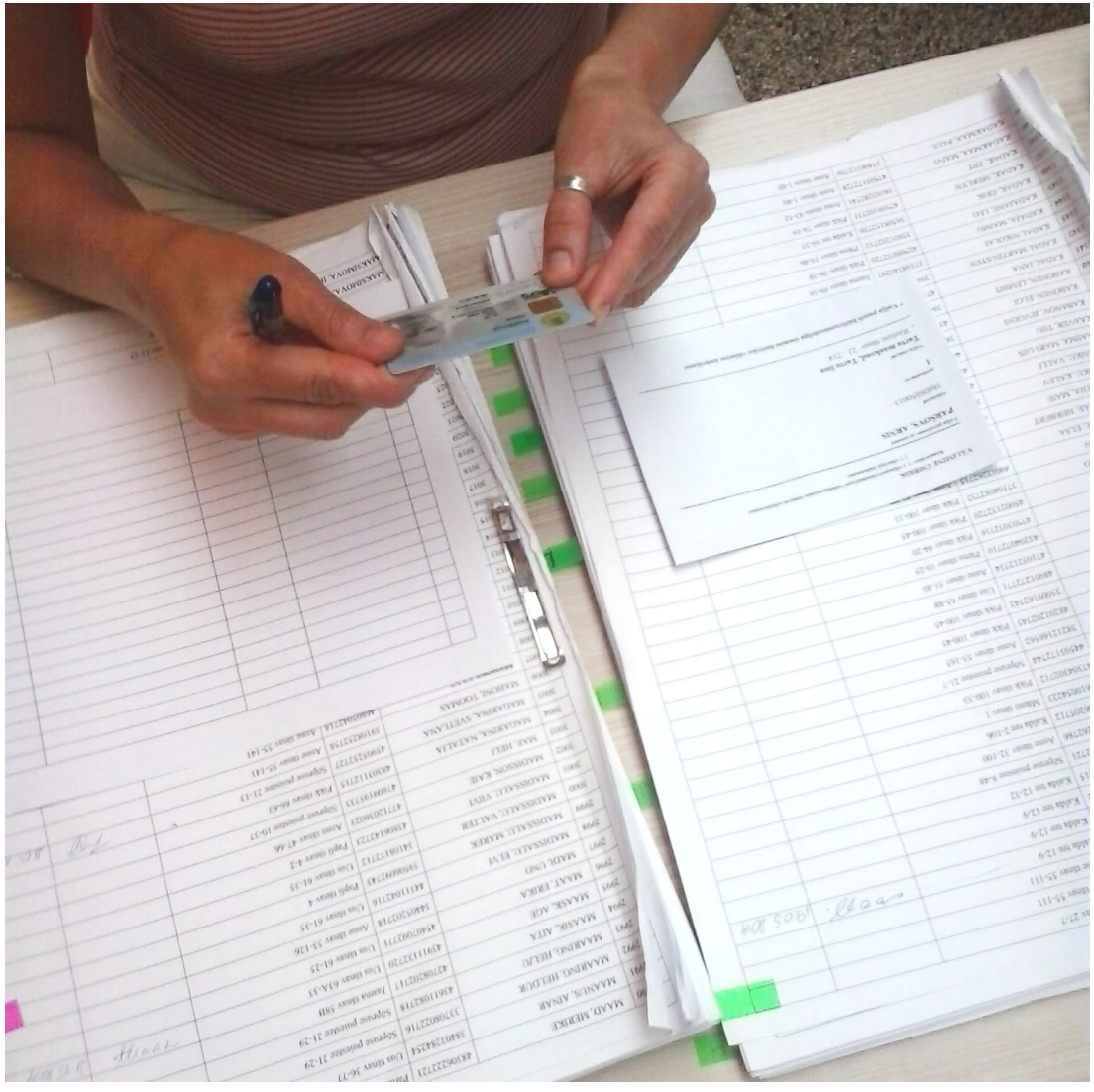


https://twitter.com/LauriBambus/status/568355079318835200/photo/1

First voting session seen as revoting

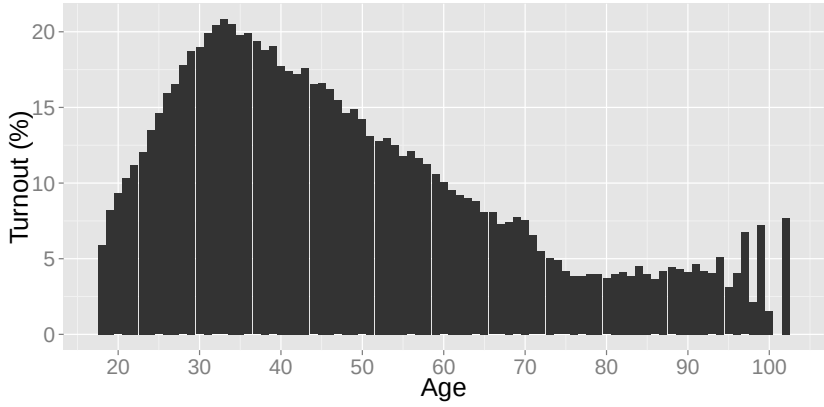
Security feature. No cases have been registered by the NEC.

Non-i-voter denied paper vote



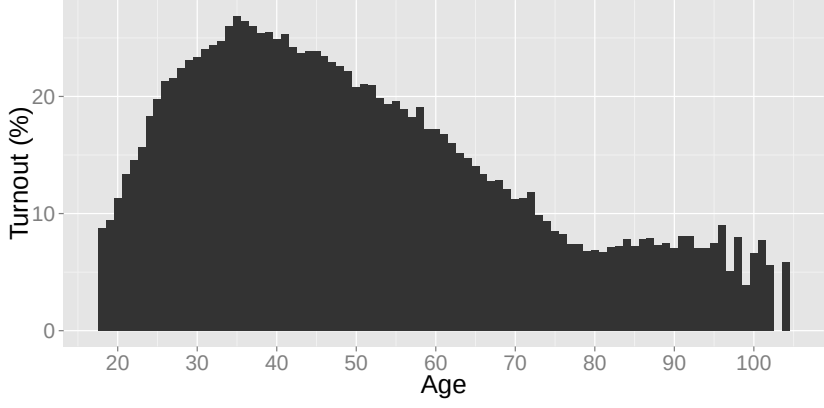
On election Sunday I-voter will be denied paper vote.
Security feature. No cases have been registered by the NEC.

General statistics – voter activity by age



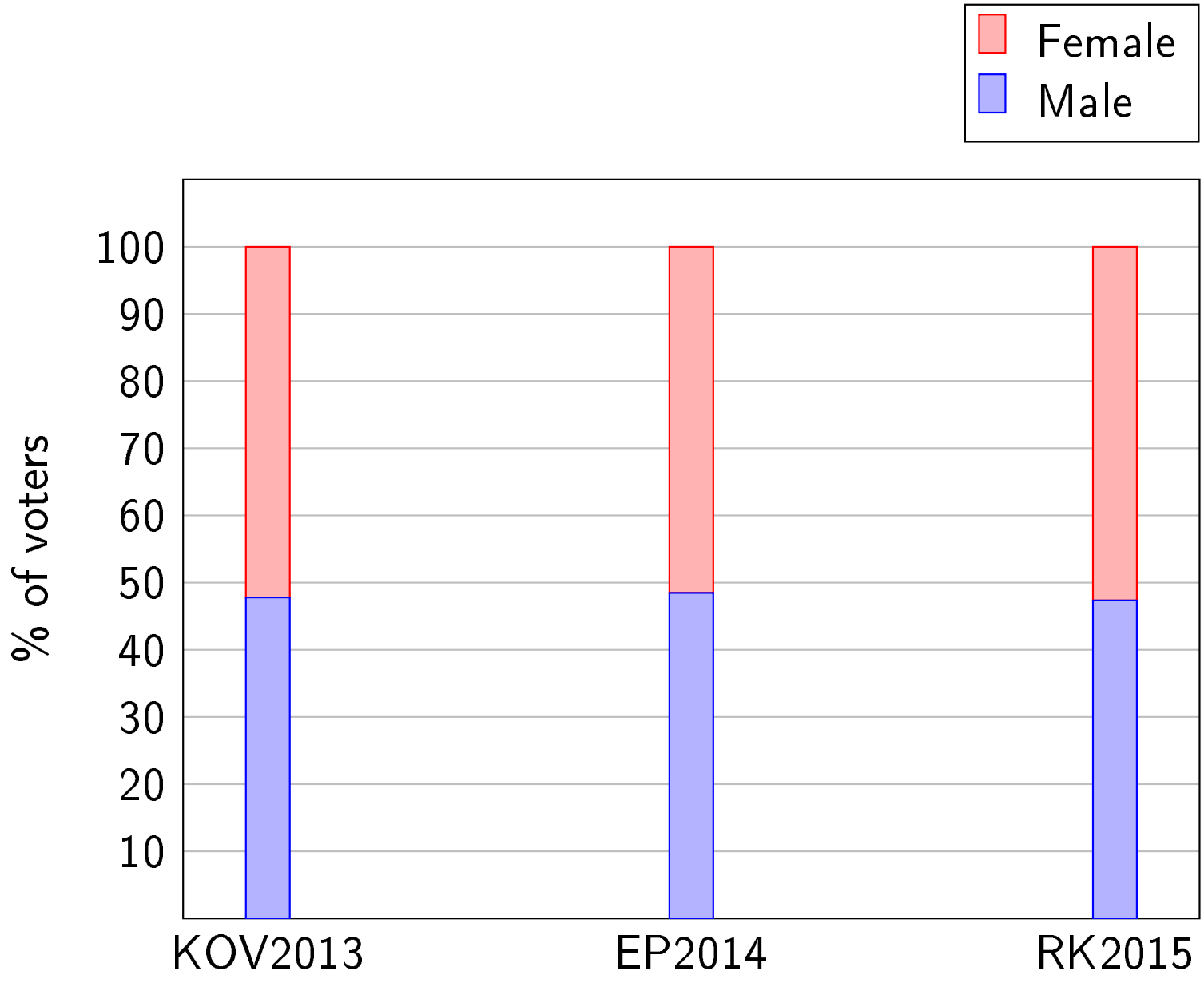
KOV2013

EP2014

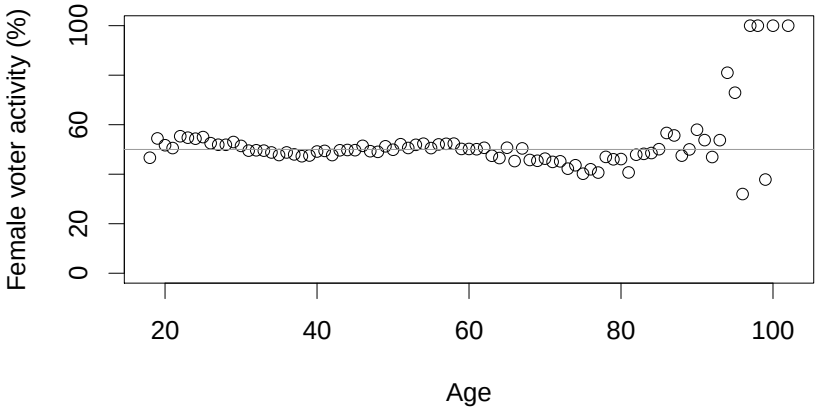


RK2015

General statistics – gender distribution of voting

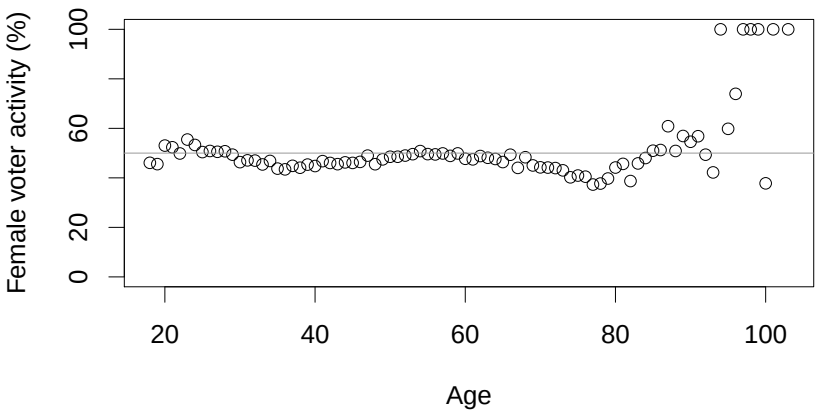


General statistics – gender distribution by age (out of i-voters)



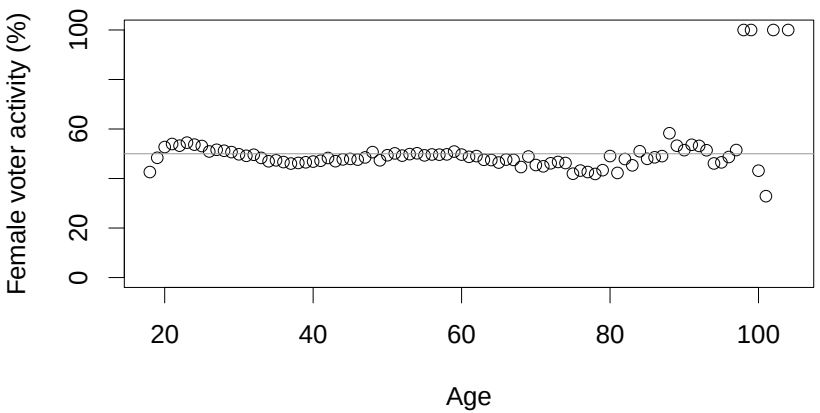
In KOV2013 I-voted:

- M: 12.94%
- F: 11.78%



In EP2014 I-voted:

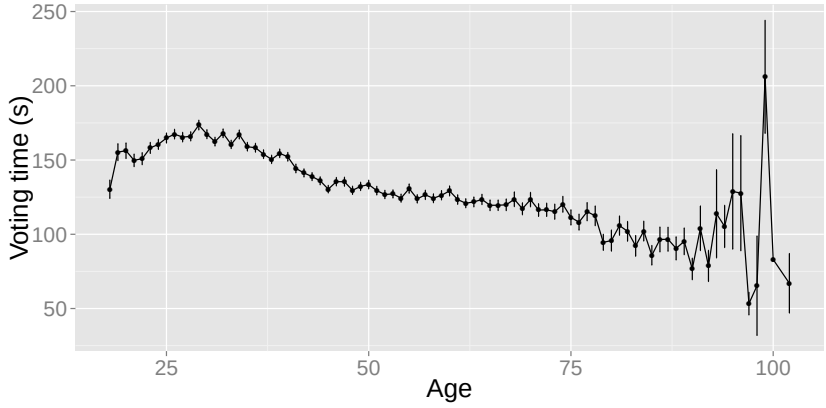
- M: 11.55%
- F: 9.84%



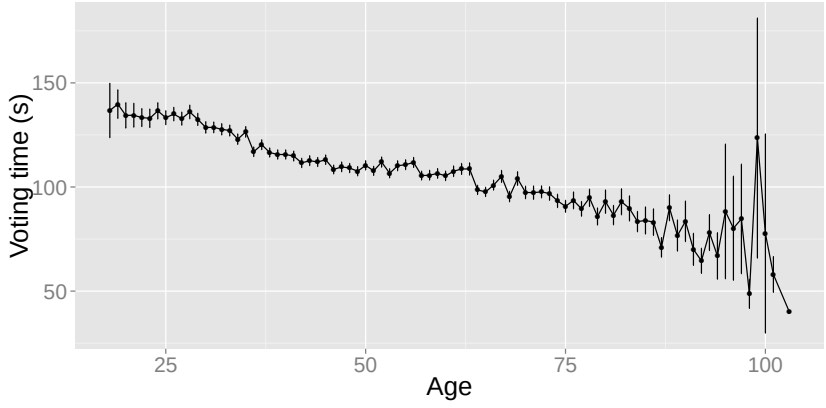
In RK2015 I-voted:

- M: 19.54%
- F: 17.40%

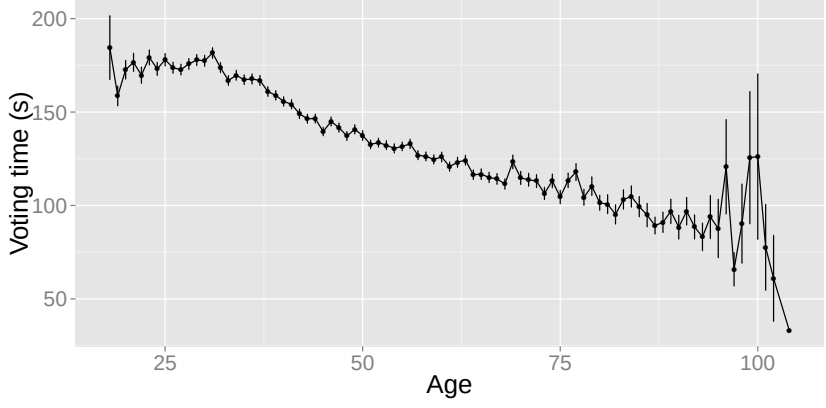
General statistics – age vs voting time



KOV2013

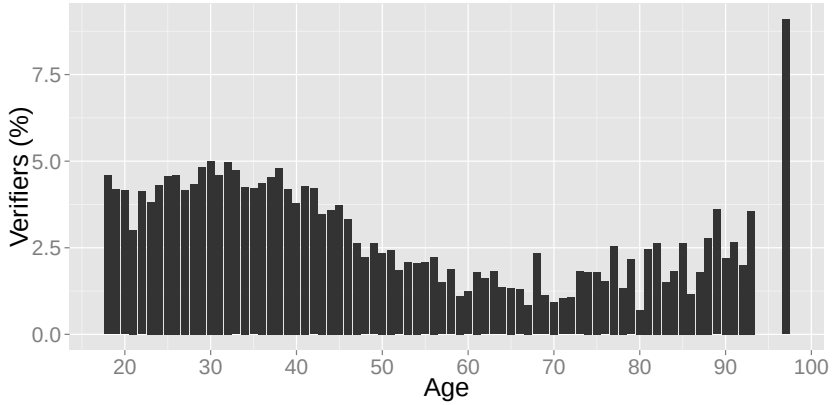


EP2014

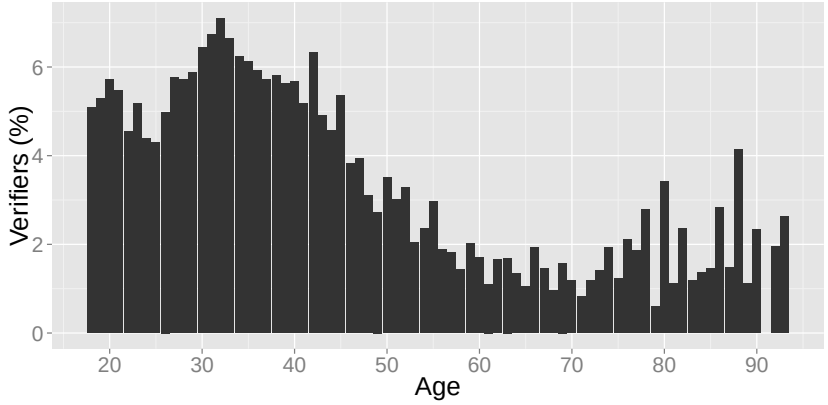


RK2015

General statistics – verifier activity by age



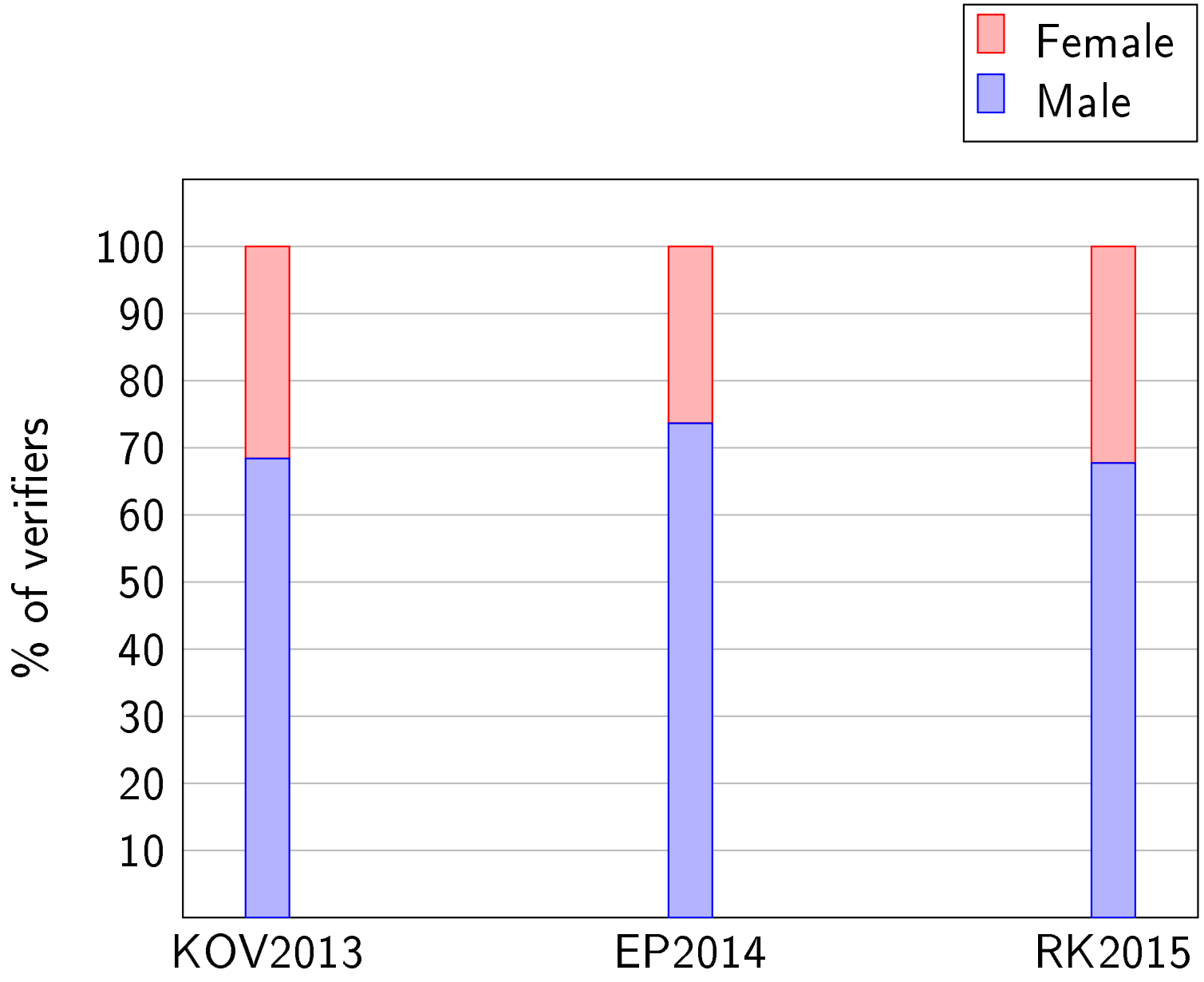
KOV2013



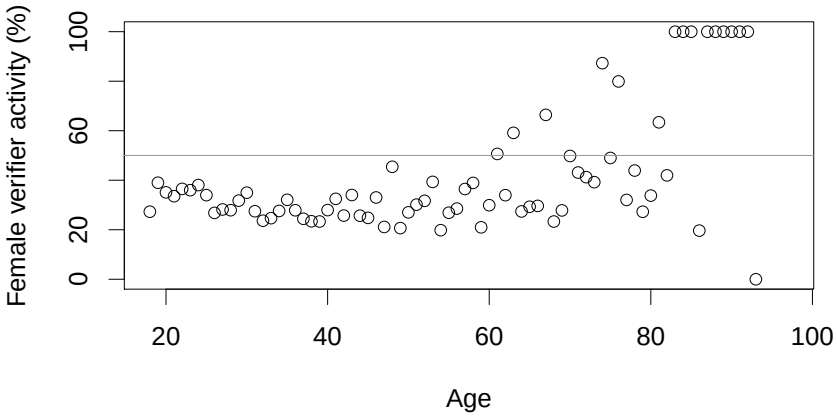
EP2014

RK2015

General statistics – gender distribution of verification

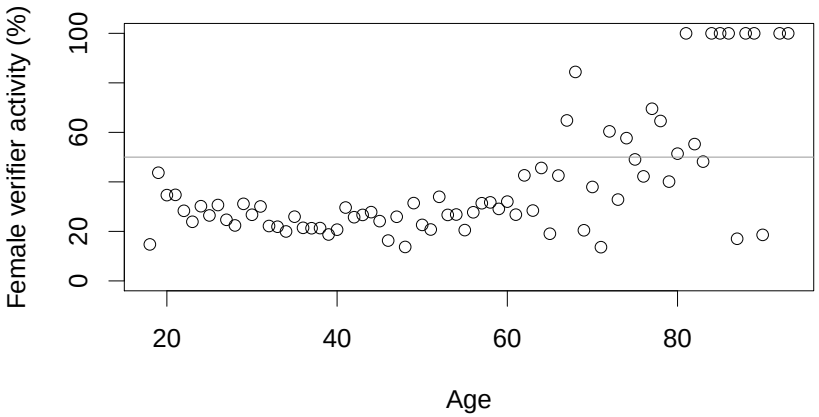


General statistics – verifier activity by gender



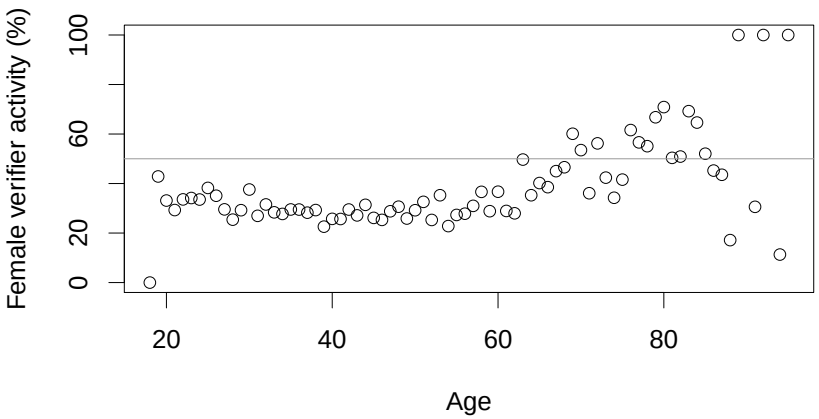
In KOV2013 verified:

- M: 4.87%
- F: 2.04%



In EP2014 verified:

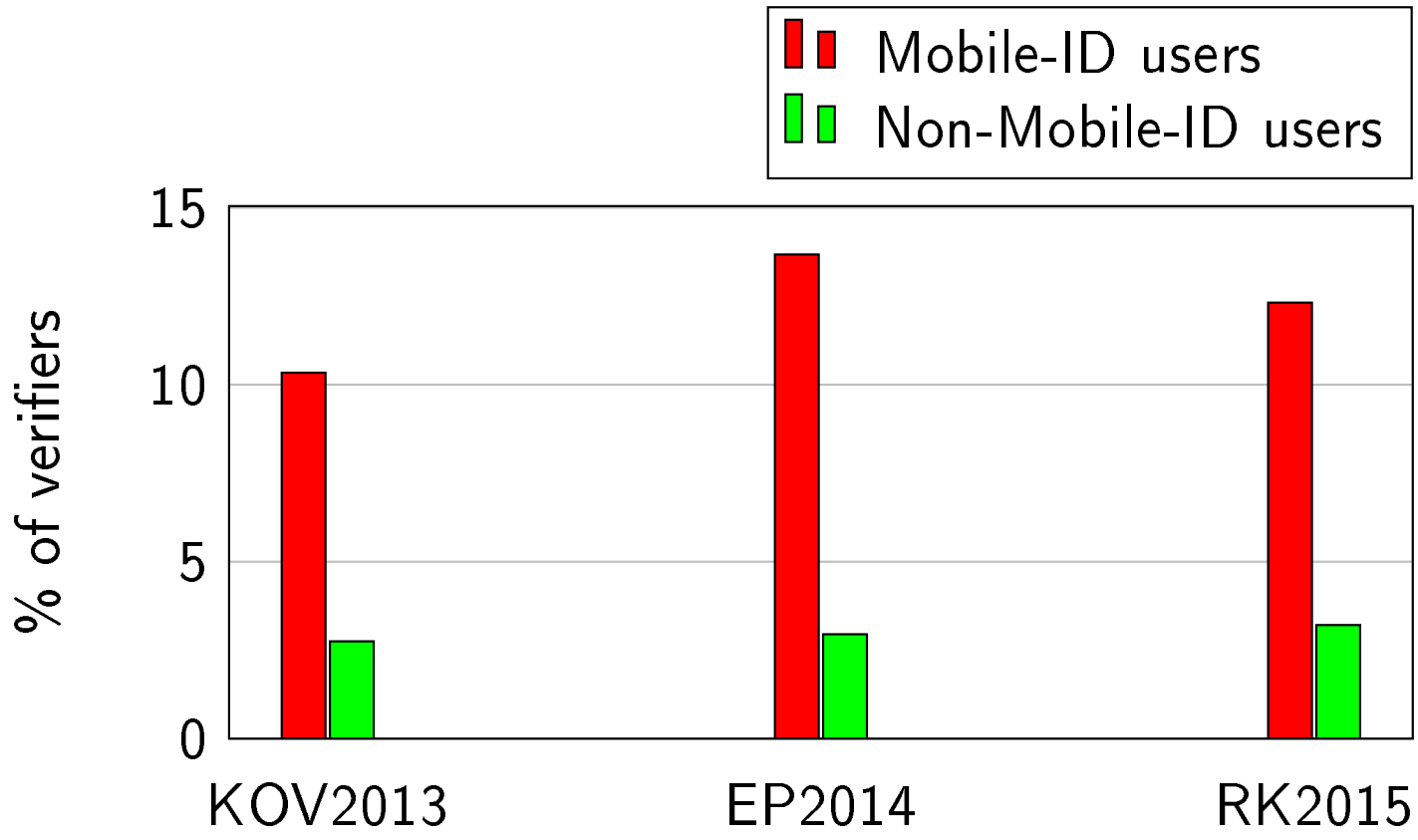
- M: 6.26%
- F: 2.11%



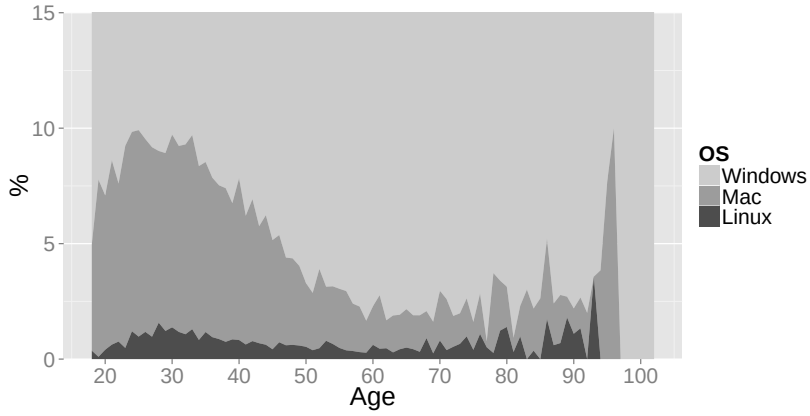
In RK2015 verified:

- M: 6.16%
- F: 2.64%

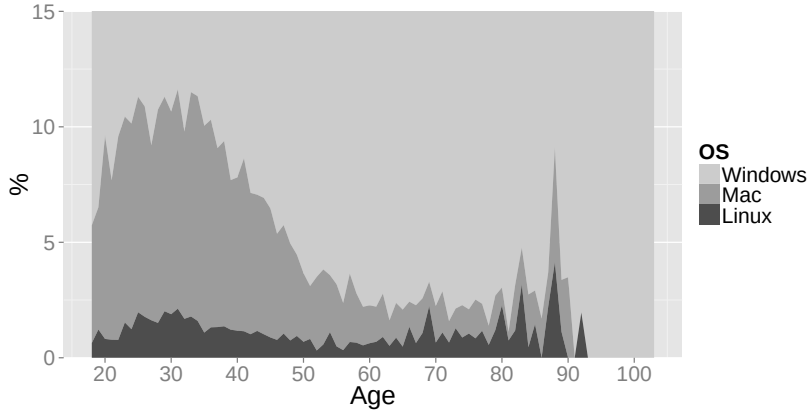
Verification activity among Mobile-ID users



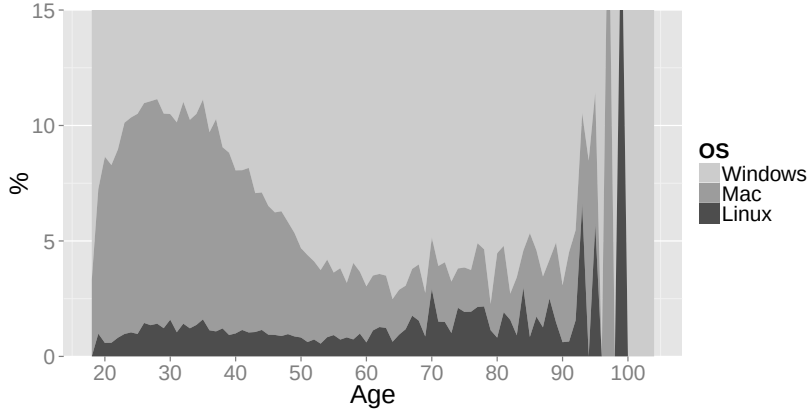
General statistics – OS popularity by age



KOV2013

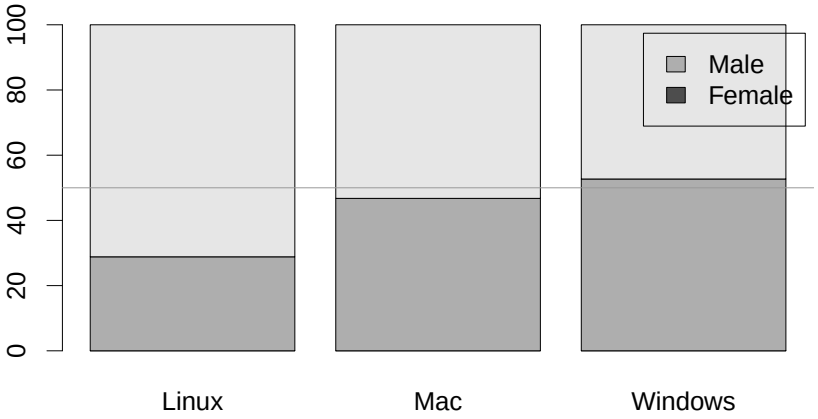


EP2014

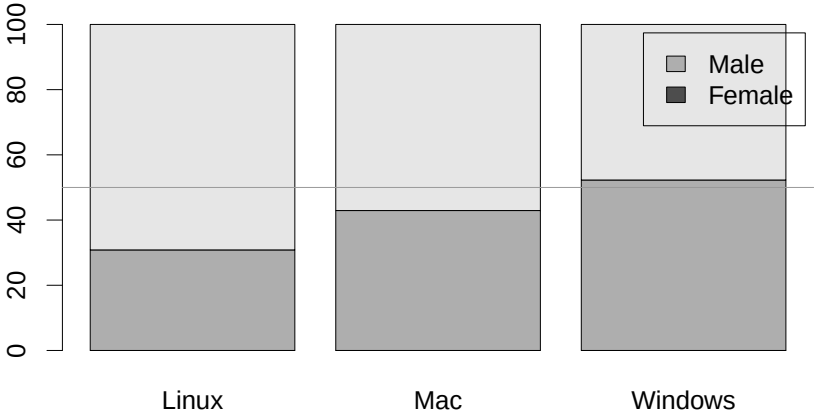


RK2015

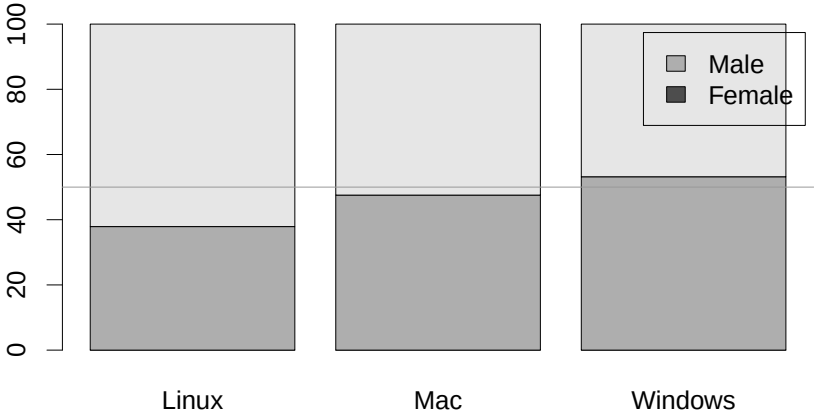
General statistics – OS popularity by gender



KOV2013

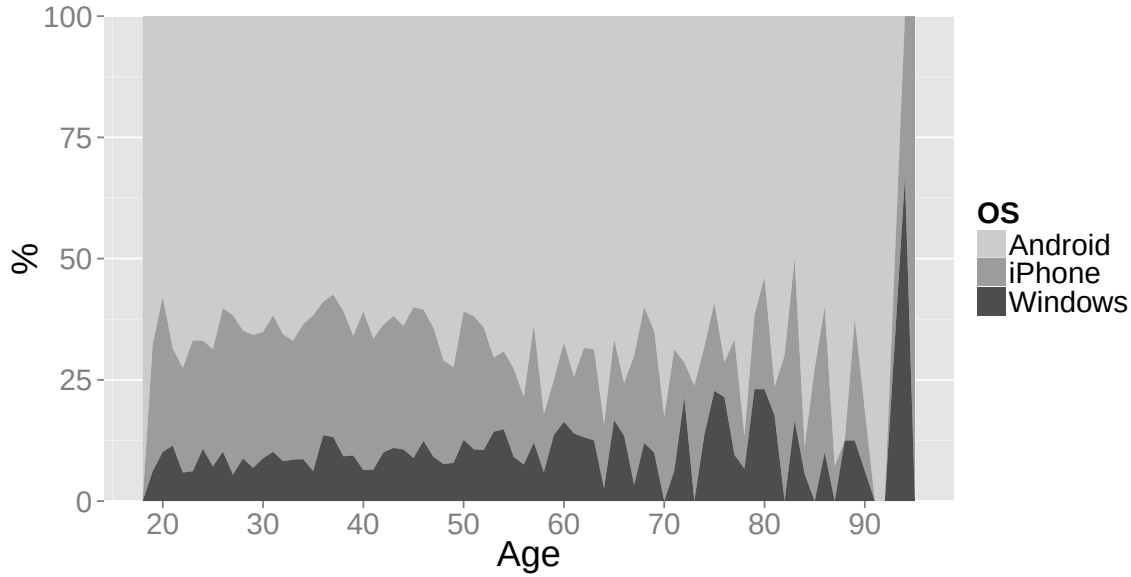


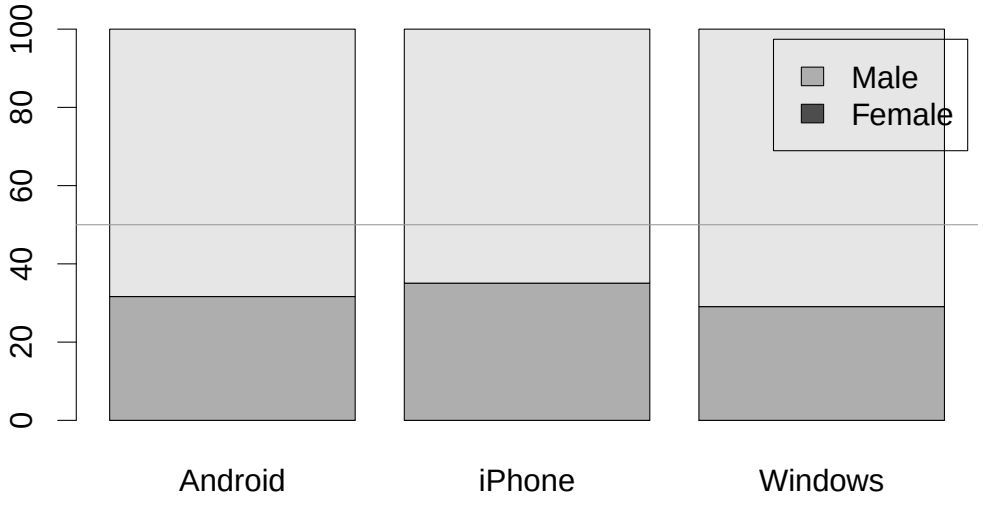
EP2014



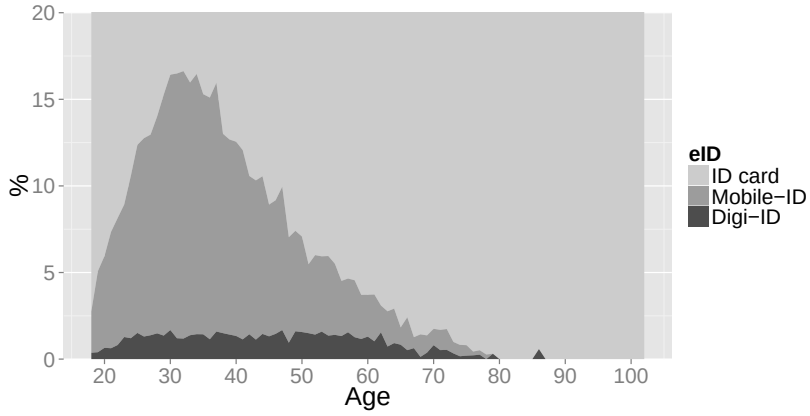
RK2015

General statistics – Verification OS popularity (RK2015)

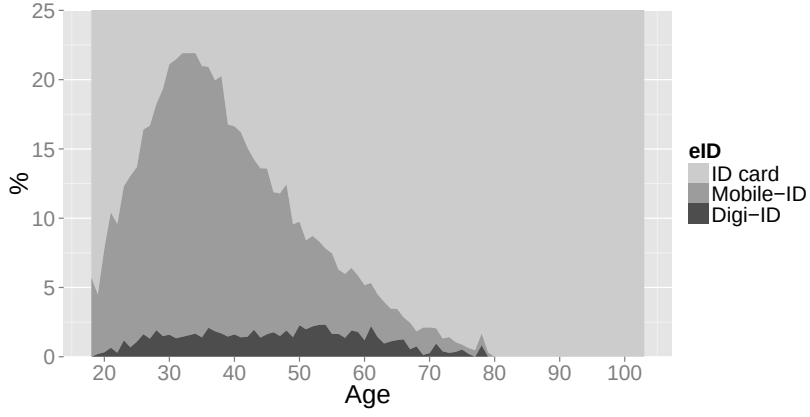




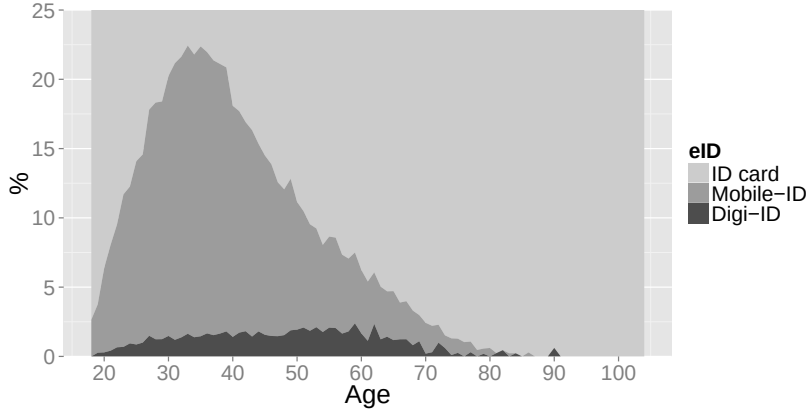
General statistics – eID tool popularity by age



KOV2013

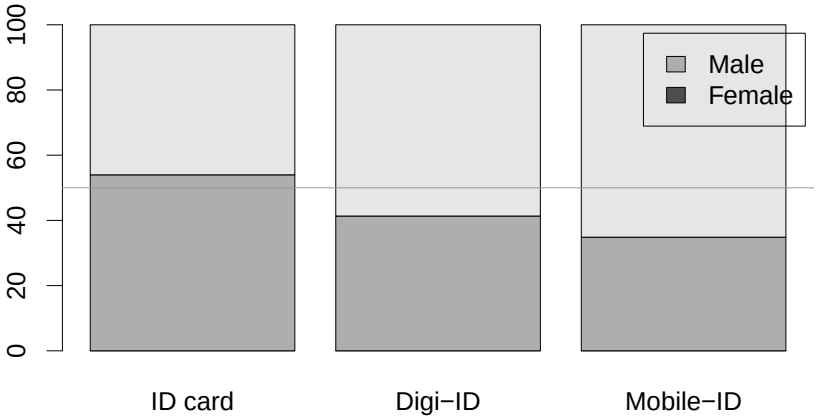


EP2014

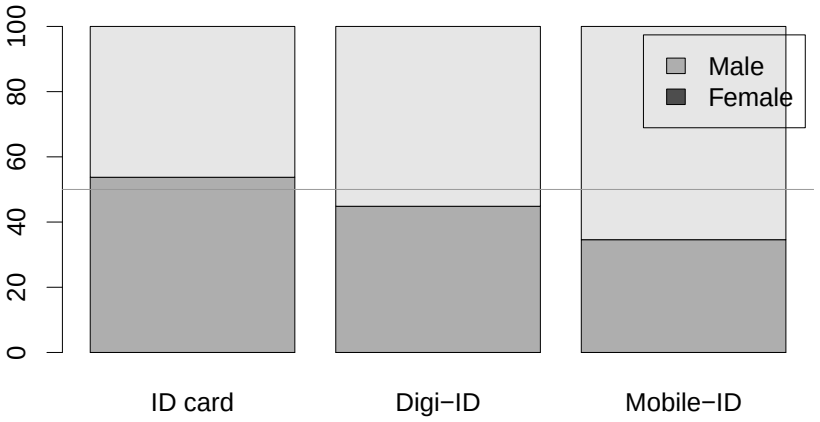


RK2015

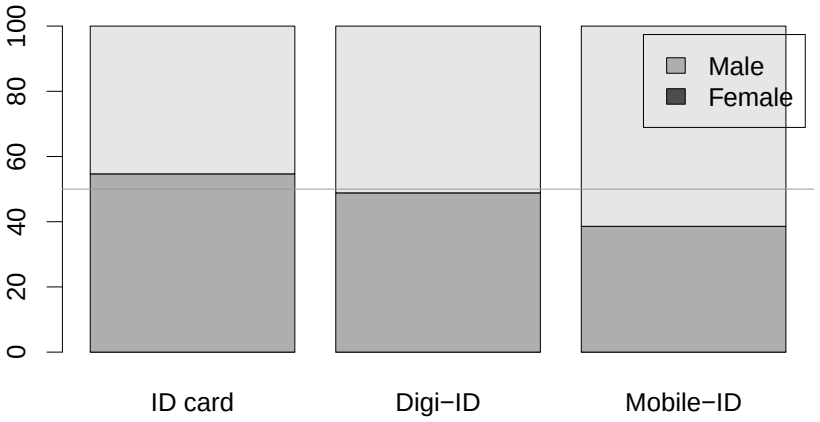
General statistics – eID tool popularity by gender



KOV2013



EP2014



RK2015

Conclusions

- Systematic data analysis method has been developed
- Several bugs were found and fixed
- No large-scale attacks were detected against the i-voters
- Observations are similar between the elections
- Interesting phenomena were observed
- Limitations
  - Some data not available for investigation
  - Attack vs legitimate behaviour
  - Unexplained voter behaviour